

Using a Client-Based Sandbox to Defend Against Zero-day



Transformation
through Partnerships

A Case Study

Jerich Beason - Cyber Security Program Manager, Lockheed Martin

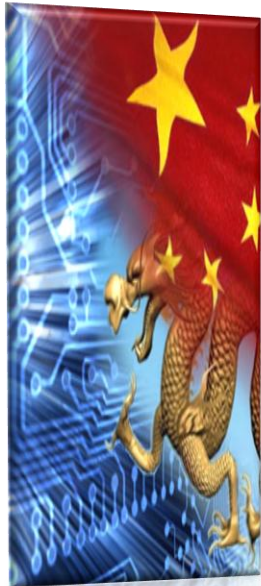
Suramie Ryan - Sr. Information Assurance Engineer, Lockheed Martin

4/18/2012

- **Mission:** Provide high-caliber protective force, security engineering, technical, and support services to safeguard and secure special nuclear material, personnel, property, and information in support of the Department of Energy, National Nuclear Security Administration Nevada Site Office operations
- **Program Scope**
 - 320 employees
 - 300 PCs
 - 40 Servers (VMWare, Exchange, BES, DNS etc..)

What's the Problem?

Nation States



Motives include:

- Cyber Espionage
- Intellectual Property Theft
- Probing of Critical Infrastructures

Cyber Criminals



Motives include:

- Identity Theft
- Corporate financial fraud
- Black Market Sales to Nation States
- Probing of Financial Infrastructures

Hacktivists



Motives include:

- Political Action
- Shaming the government
- Exposing Government Secrets
- Lulz

The Target Keeps Moving

80,000 Daily*

New Malware Variants

The #1 Attack Vector = **The User**

30,000 Daily**

Infected Websites – 80% legitimate

* McAfee 3rd Quarter 2011 Threat Report

** Sophos Security Threat Report 2012



Root Cause Analysis - The Unwitting Accomplices

- Ubiquitous usage of Internet and Email has enabled adversaries to shift tactics
- Prey on human psychology
 - Spear Phishing
 - Drive by Downloads
 - Malicious sites
 - Hijacked trusted sites
 - Malvertising
 - Trust in social networks
 - Facebook and Twitter worms (click-jacks)
 - Faith in Internet search engines
 - Poisoned SEO
 - User Initiated Infections
 - Fake A/V and fear mongering



Existing Defenses are Inadequate

Firewalls

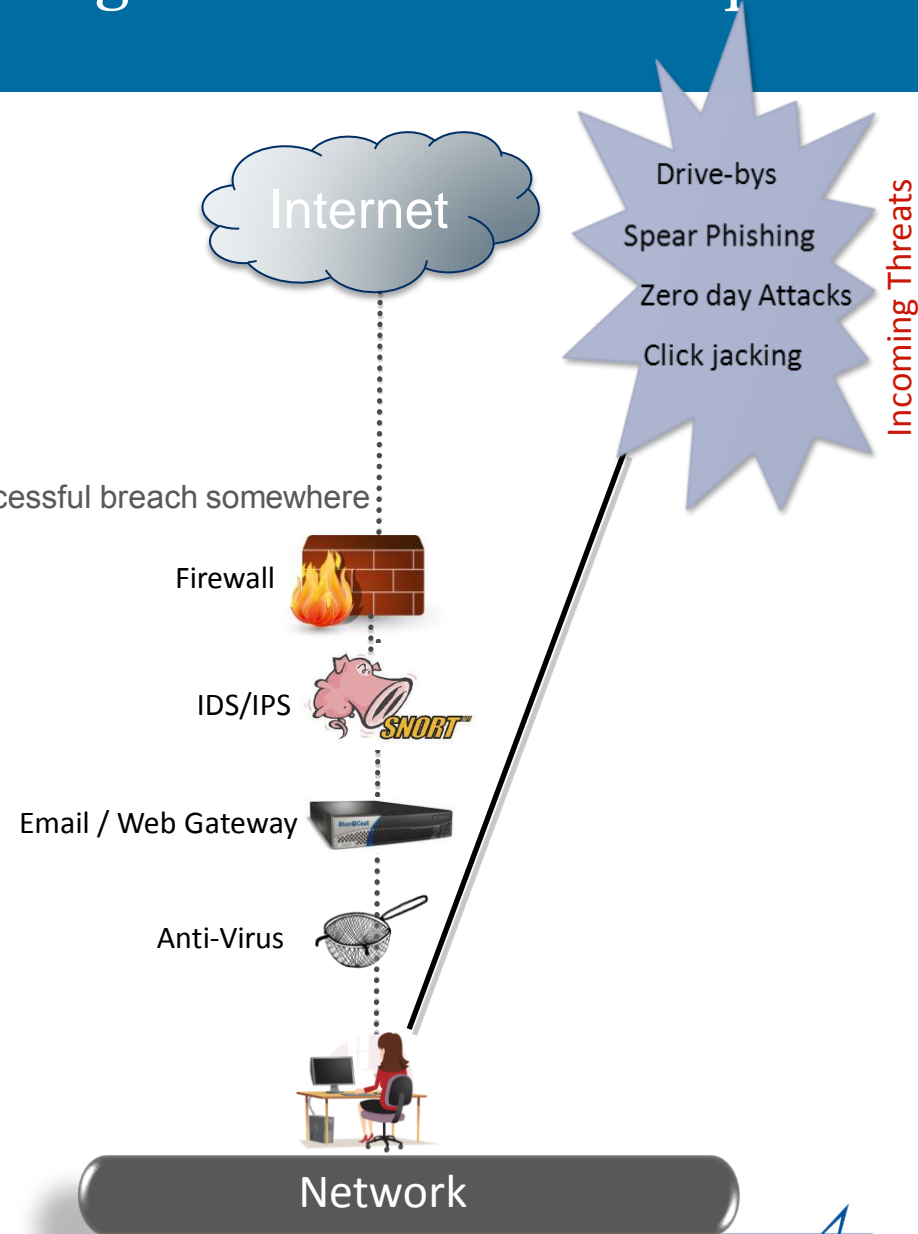
- Do not stop Web and Email traffic
- Only stops “known bad” url requests

Email / Network Gateways

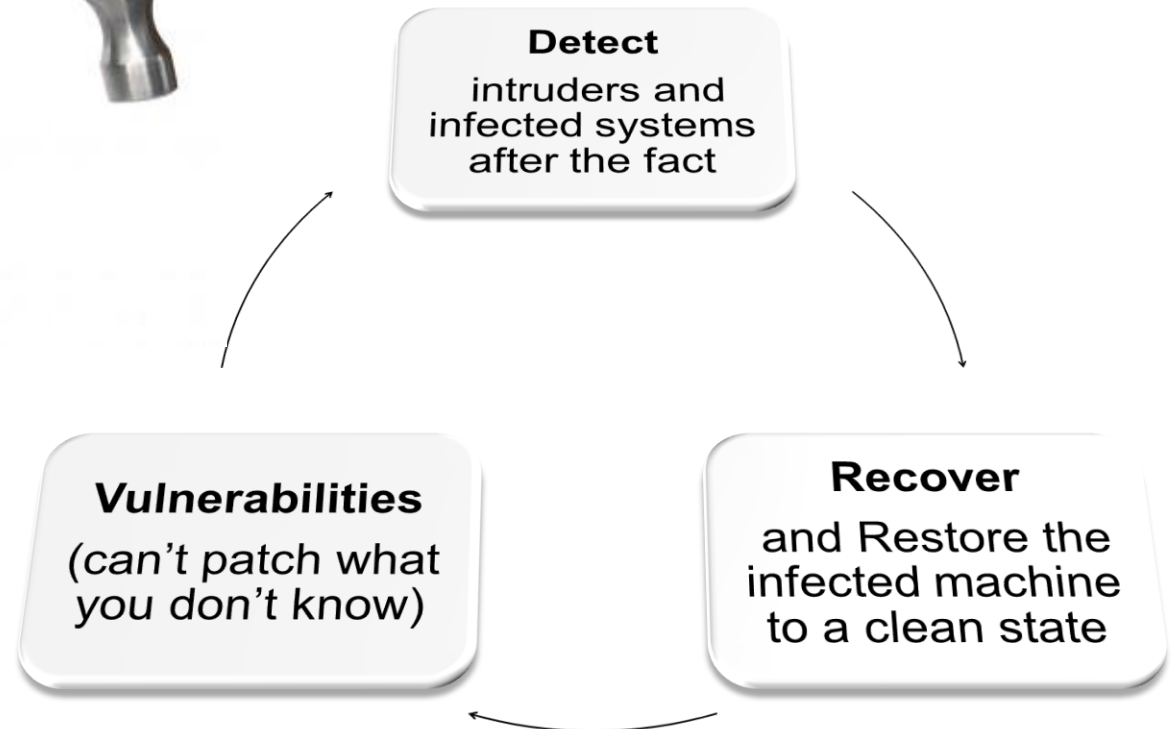
- Requires signatures of “known bad” which means a successful breach somewhere
- Choke-point for Web traffic – scale?
- Misses malware requiring human interaction

Anti-virus

- Requires signatures of “known bad”
- Signature updates lag by days/weeks
- Malware built to avoid AV detection



Time to Break The Cycle



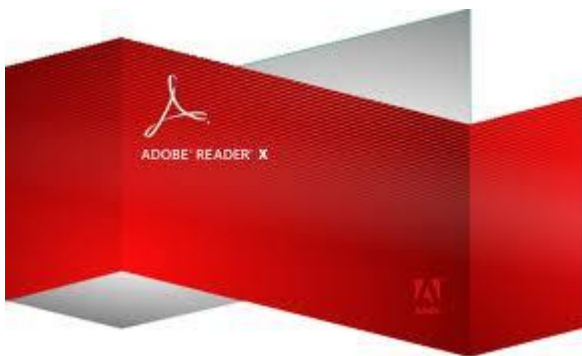
Solution

Protect the users from themselves in a sandbox

- A security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third-parties, suppliers, untrusted users and untrusted websites
- Allows you to witness the execution path of malware samples
- Allows you to identify potential call back domains and IP addresses



Potential Sandbox Solutions Evaluated



Google Chrome



- **Host containment** of processes, the file system, and the OS kernel
- **Network containment** to prevent the untrusted instances of the application from accessing file shares or other internal networked systems that contain critical data
- **Near real-time detection** of attack activity including zero days
- **Ease of use** and seamless integration to the host desktop environment
- **Forensics data capture** and reporting

	Host Containment	Network Containment	Near Real Time Detection	Usability	Forensics data Capture	Easily Deployed and Managed	Price
 Google Chrome		✓		✓		✓	✓
		✓		✓		✓	✓
invincea™	✓	✓	✓	✓	✓	✓	
		✓	✓	✓	✓	✓	

This score card is based on the results of the tests conducted and is not intended to be a depiction of actual functionality of the products discussed

Broad Set of Attack Vectors



Web

- Invincea Browser Protection becomes default desktop browser and default URL handler
 - **Protect Against:** Drive-by downloads, poisoned SEO, fake A/V, hijacked sites, social network worms (click-jacks)
-



Email

- DocumentProtection handles inbound attachments
 - PDF, zip files, and executables
 - **Protect Against:** Anything from spear-phishing to drive-by downloads, self-extracting zip files, malicious executables, weaponized PDFs
-

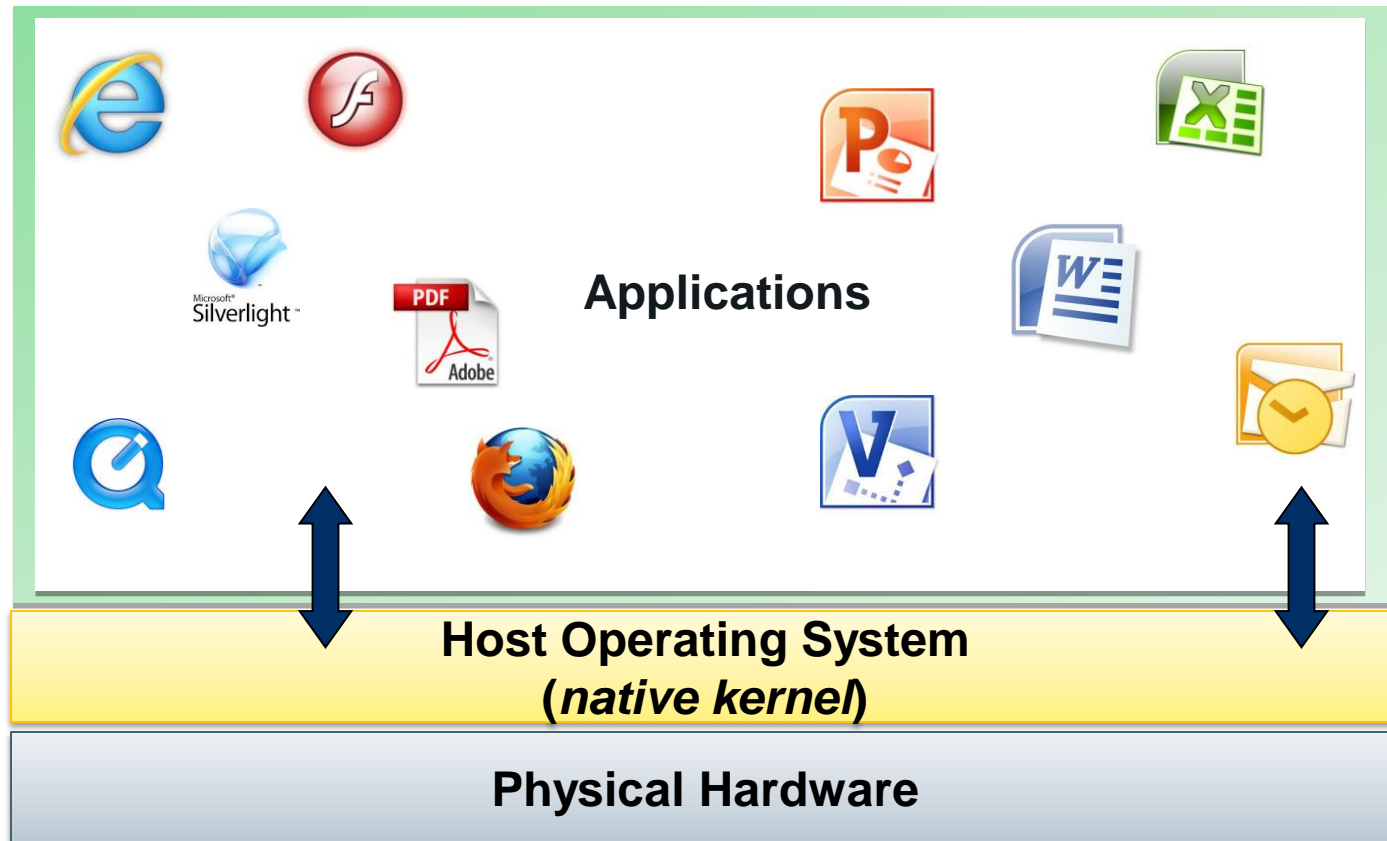


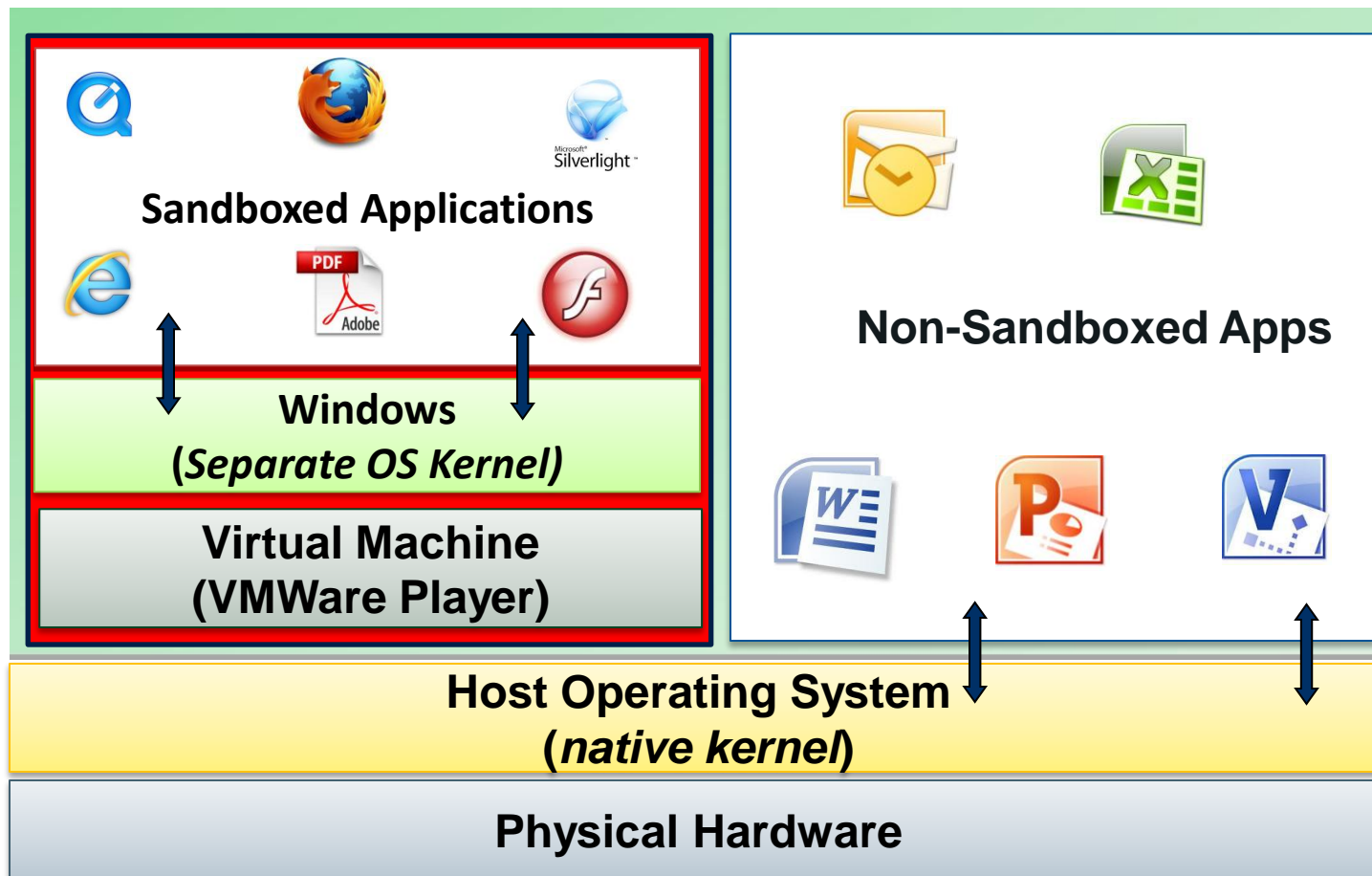
External Drive

- DocumentProtection runs USB file attachments
 - PDF, zip files, and executables
 - **Protect Against:** Self-extracting zip files, malicious executables, weaponized PDFs

Architecture

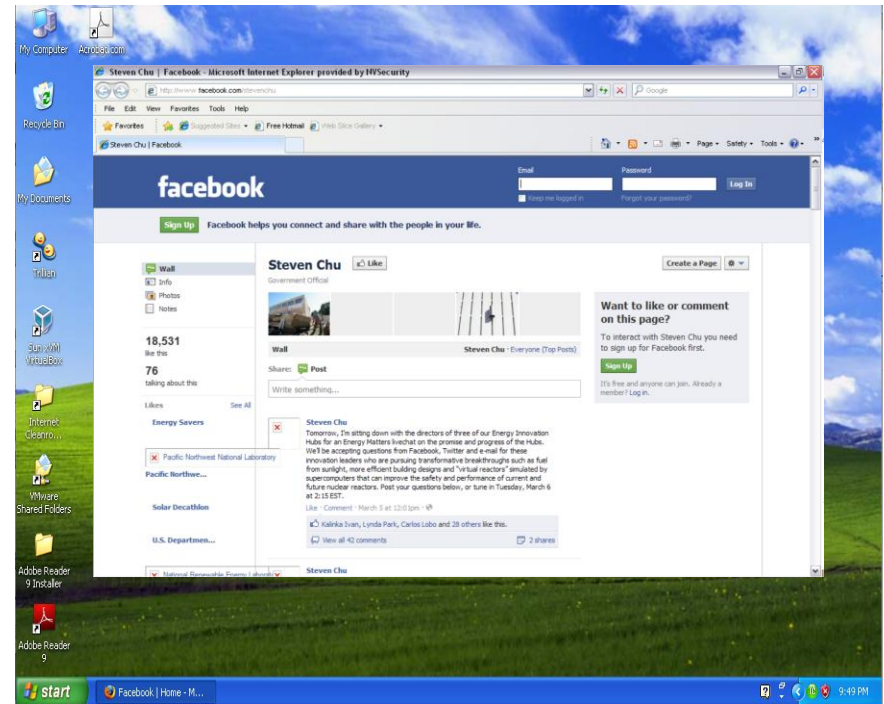
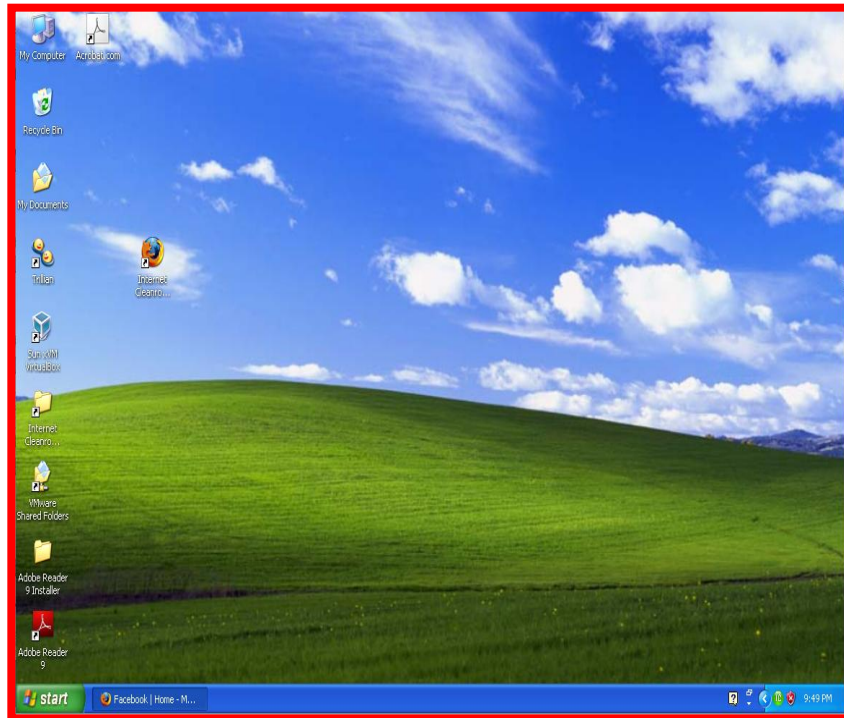
Invincea in a Virtual Machine Using VMware Player





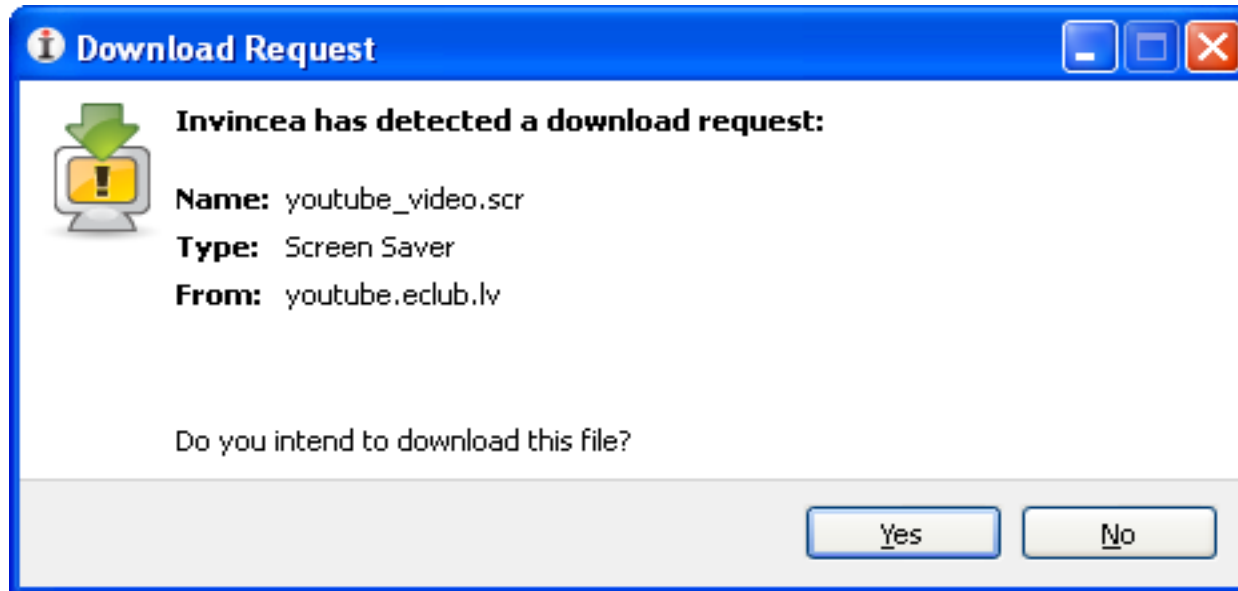
- Sandbox (guest kernel) is distinct from host system
- Infections of the virtual browser and kernel do not affect the host OS

What is a Sandbox

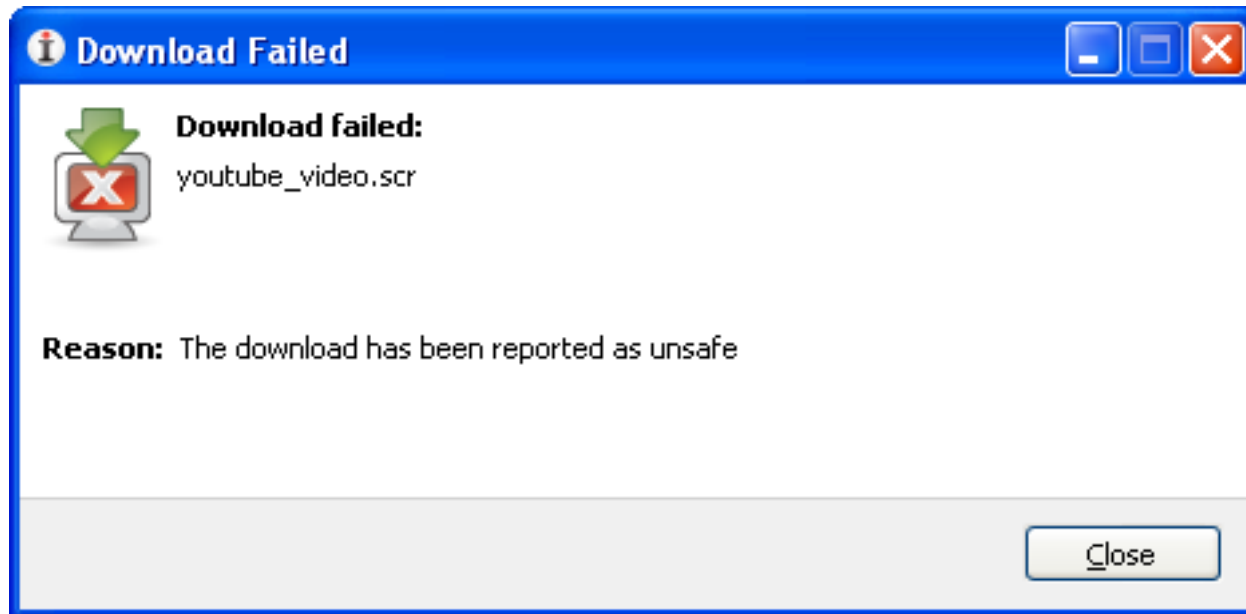




- The user attempts to download a file



- Invincea detects that this is an unsafe file and stops the download



IT Management

- Minimum system requirements
 - 2GB RAM for Windows XP, 3GB for Windows 7
- Supports IE 6-8 and Firefox on Windows XP or Windows 7
- Build the VM workstation to specifications (Adobe Reader version, Flash version etc.)
- Configurable to run dual browsers for trusted and untrusted sites
 - Create list of sites to be excluded
 - Useful in dealing with Java-based apps

- Can be deployed via EXE or MSI package using software deployment solutions (Big Fix, LANDesk, SCCM)
- Typical install – 20 minutes
- Quarterly updates are done by updating the gold image and re-pushing via software deployment solution

User Experience

- New icon in addition to Internet Explorer
- Invincea Downloads folder on the desktop
 - Files downloaded off the Internet go into a separate folder before they can be copied to the location of choice
- The browser and PDFs are now wrapped in a red shell
- Extra step in modifying PDFs
- Slight decrease in browser performance

Challenges

- Resistance to change
- Occasional issues printing PDFs
- Java-based web apps
- “mailto” links on websites do not work
- Favorites in the sandbox are not synced up with favorites in Internet Explorer
- Minor training will be needed

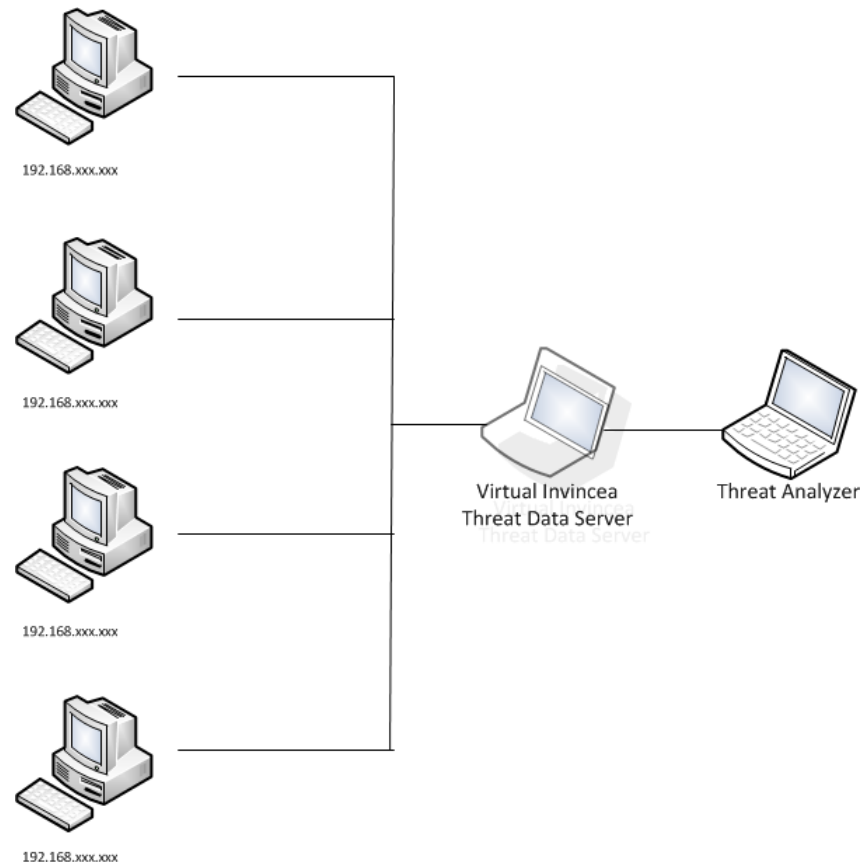
- Focus more on the developing a comprehensive white list
- Engage user population earlier on
- Identify best method for deployment (EXE vs. MSI)
- Deployment would have worked smoother if we had better standardization in our environment
 - Identify PCs with low RAM

Forensics Capability

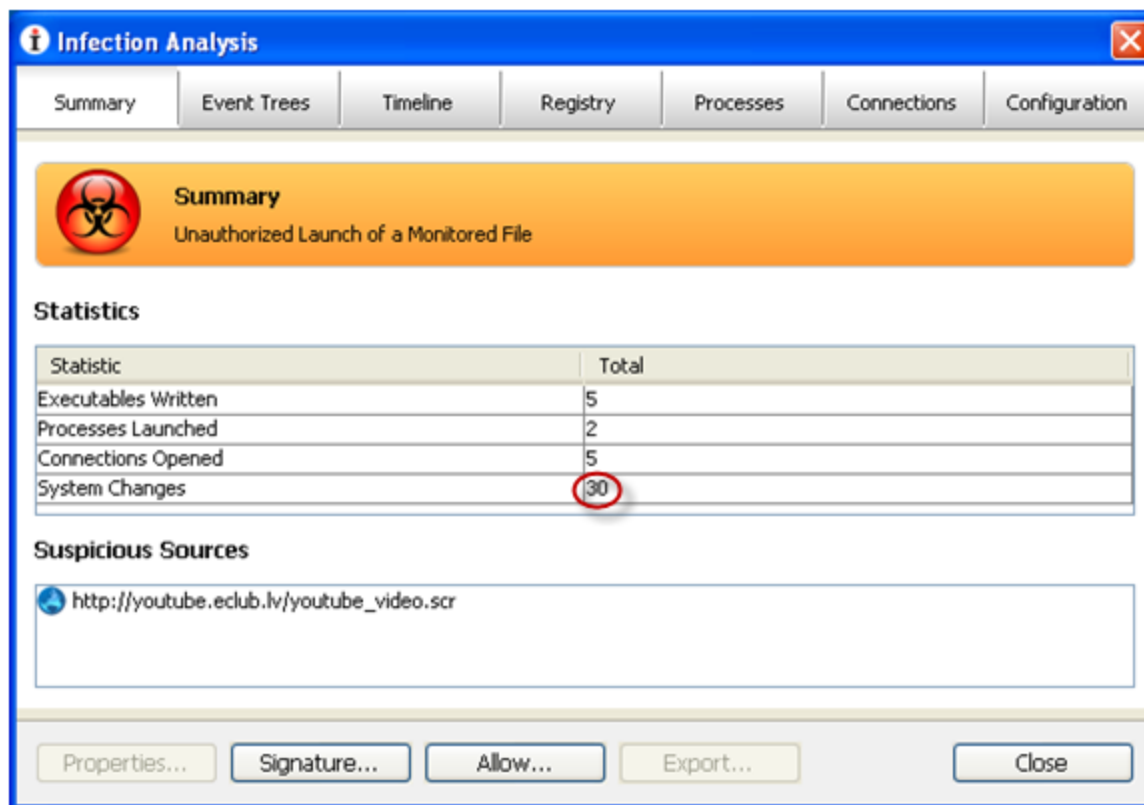
What did the malware do and how did it do it?

Activity is reported to the Threat Analyzer

- GUI that provides details on the event
- User and IP that generated the event
- Timeline of event that took place
- Registry changes attempted
- Attempts at changing or deleting processes
- Attempted connections



- Summary

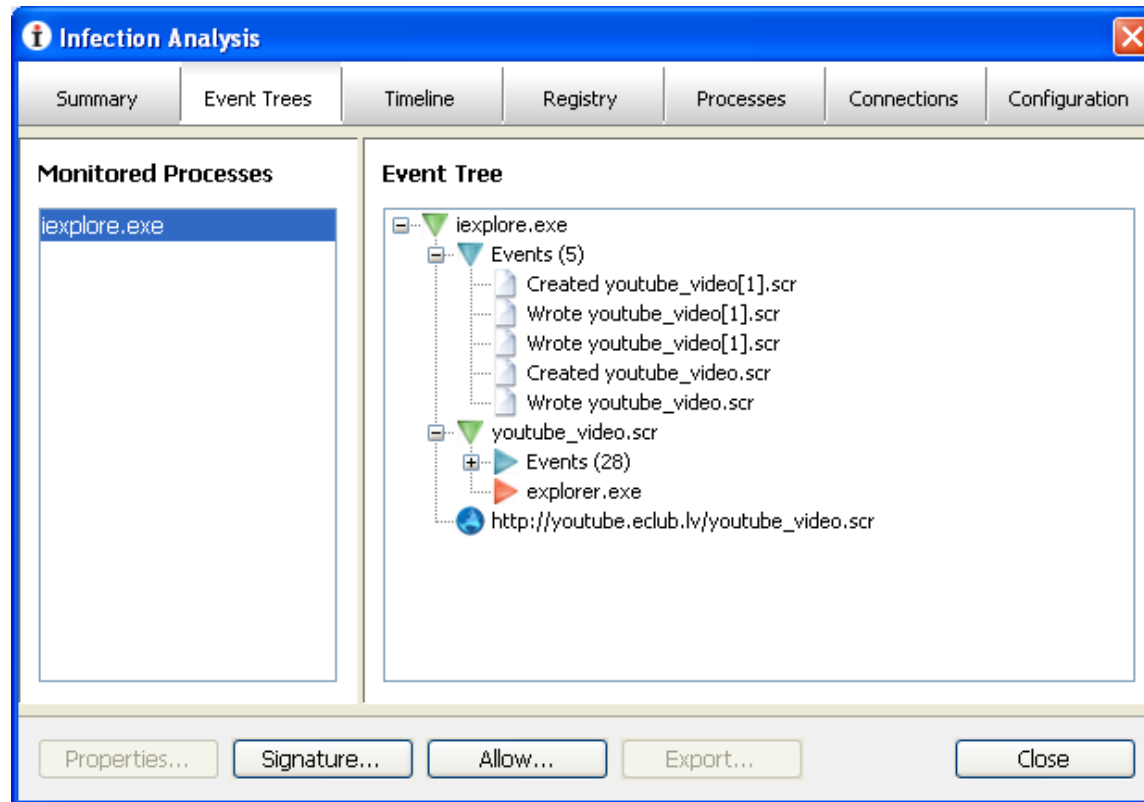


The screenshot shows the 'Infection Analysis' window with the 'Summary' tab selected. It displays a biohazard icon and the title 'Unauthorized Launch of a Monitored File'. Below this is a 'Statistics' table with the following data:

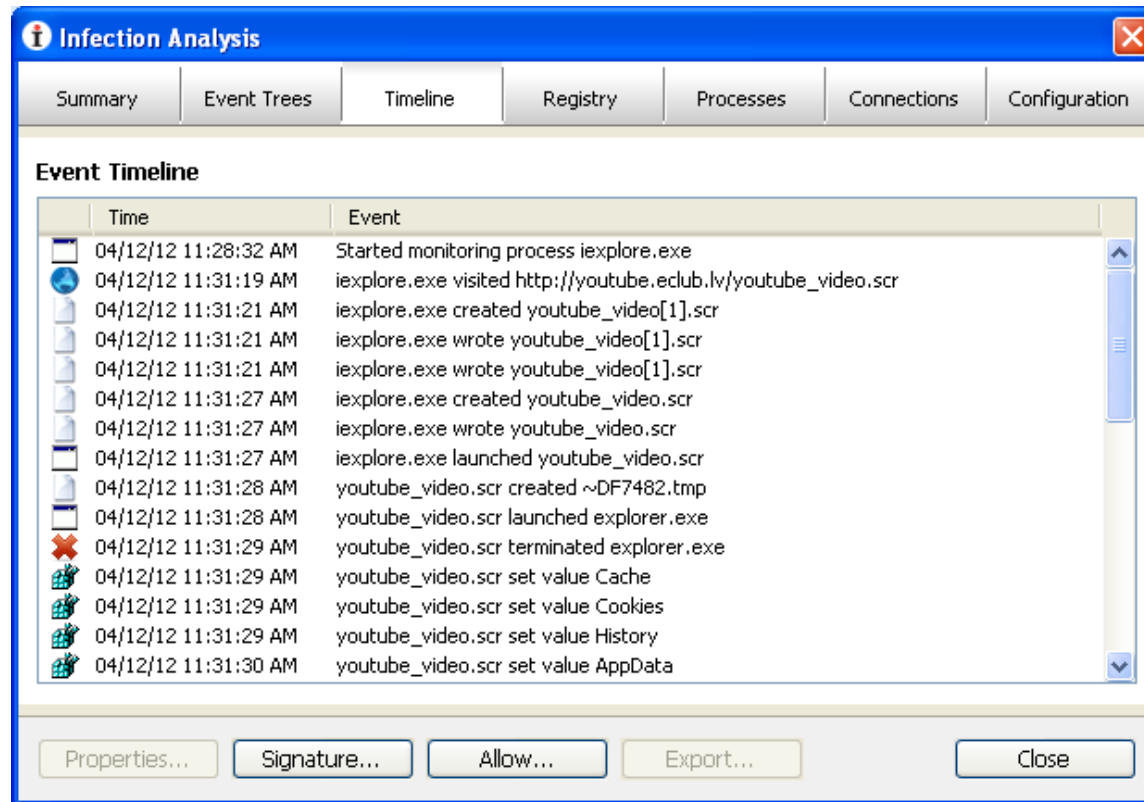
Statistic	Total
Executables Written	5
Processes Launched	2
Connections Opened	5
System Changes	30

The value '30' in the 'System Changes' row is circled in red. Below the table is a 'Suspicious Sources' section with a single entry: http://youtube.eclub.lv/youtube_video.scr. At the bottom are buttons for 'Properties...', 'Signature...', 'Allow...', 'Export...', and 'Close'.

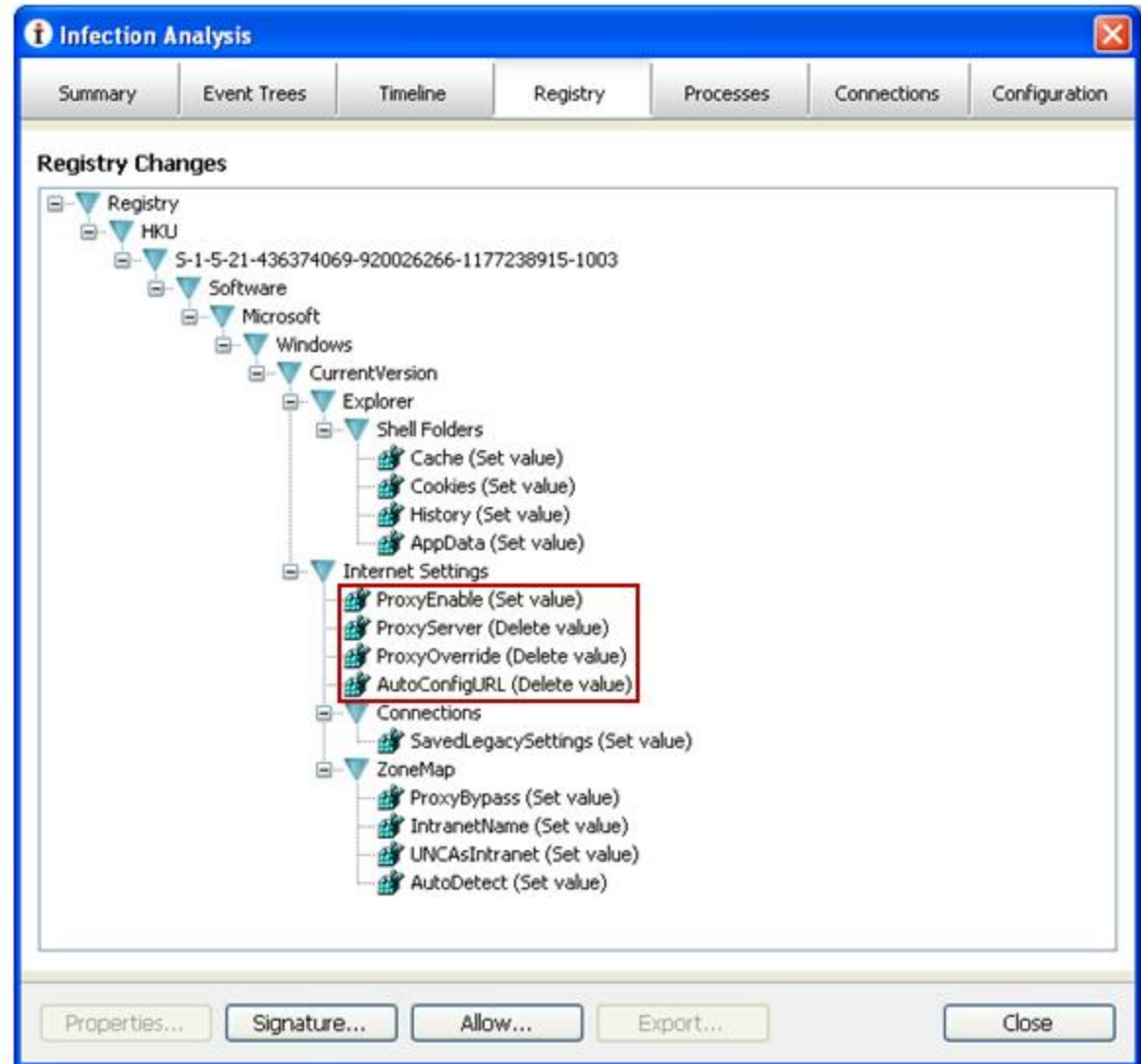
- Event Tree



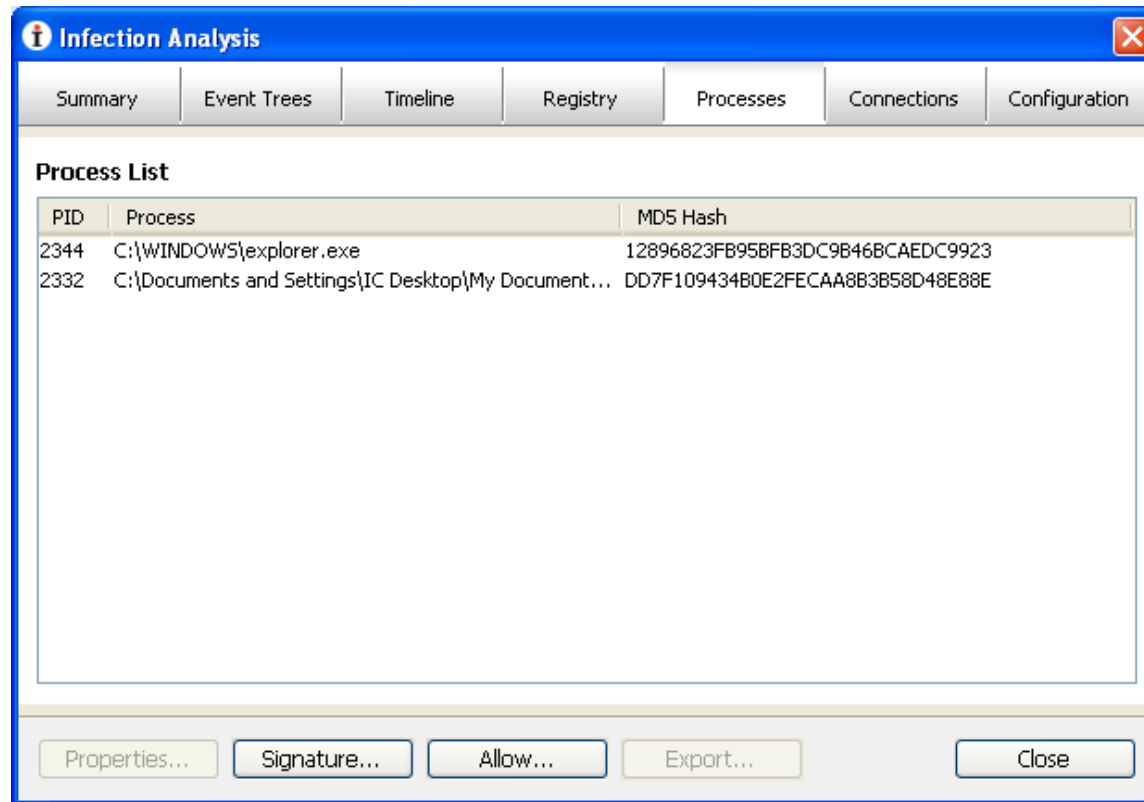
- Event Timeline



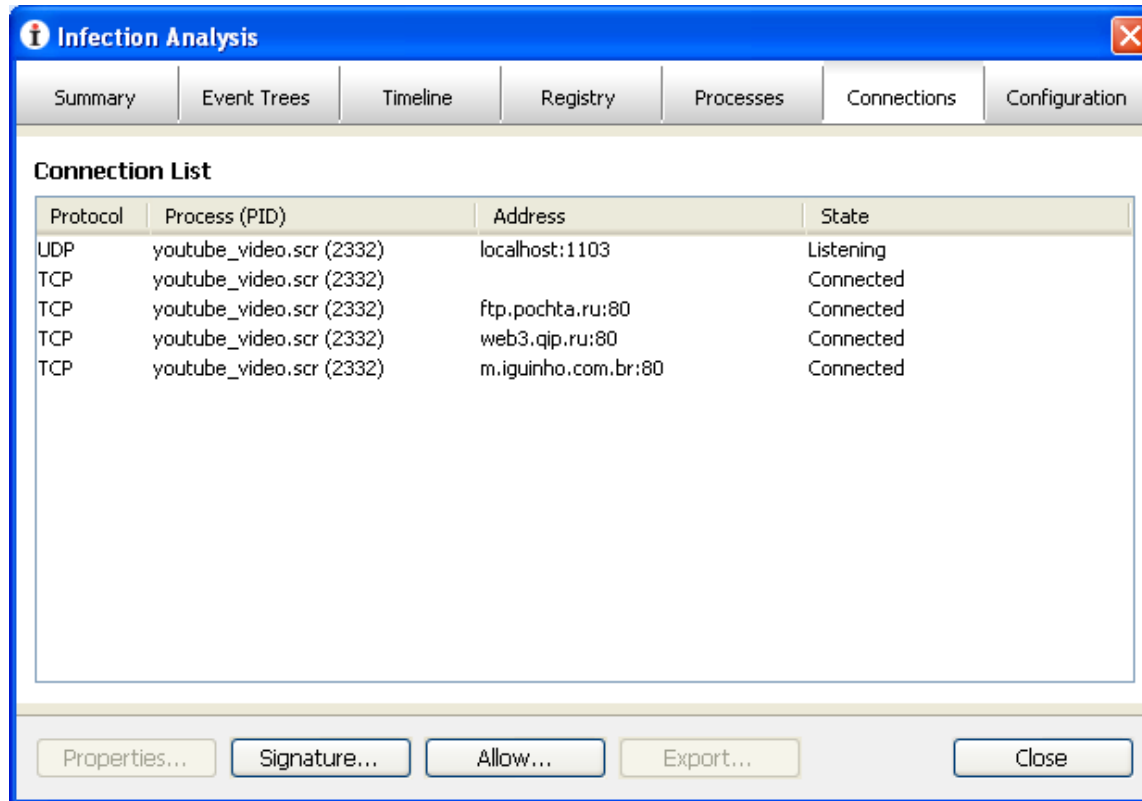
- Registry Changes



- Process List



- Connection List

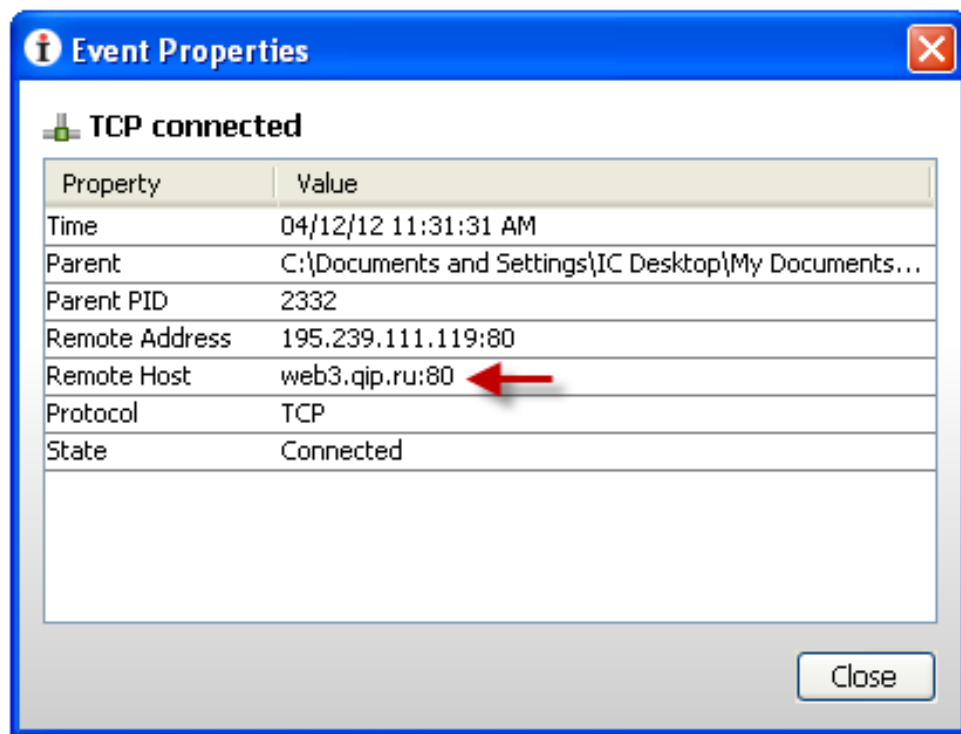


The screenshot shows the 'Infection Analysis' window with the 'Connections' tab selected. The 'Connection List' table displays the following data:

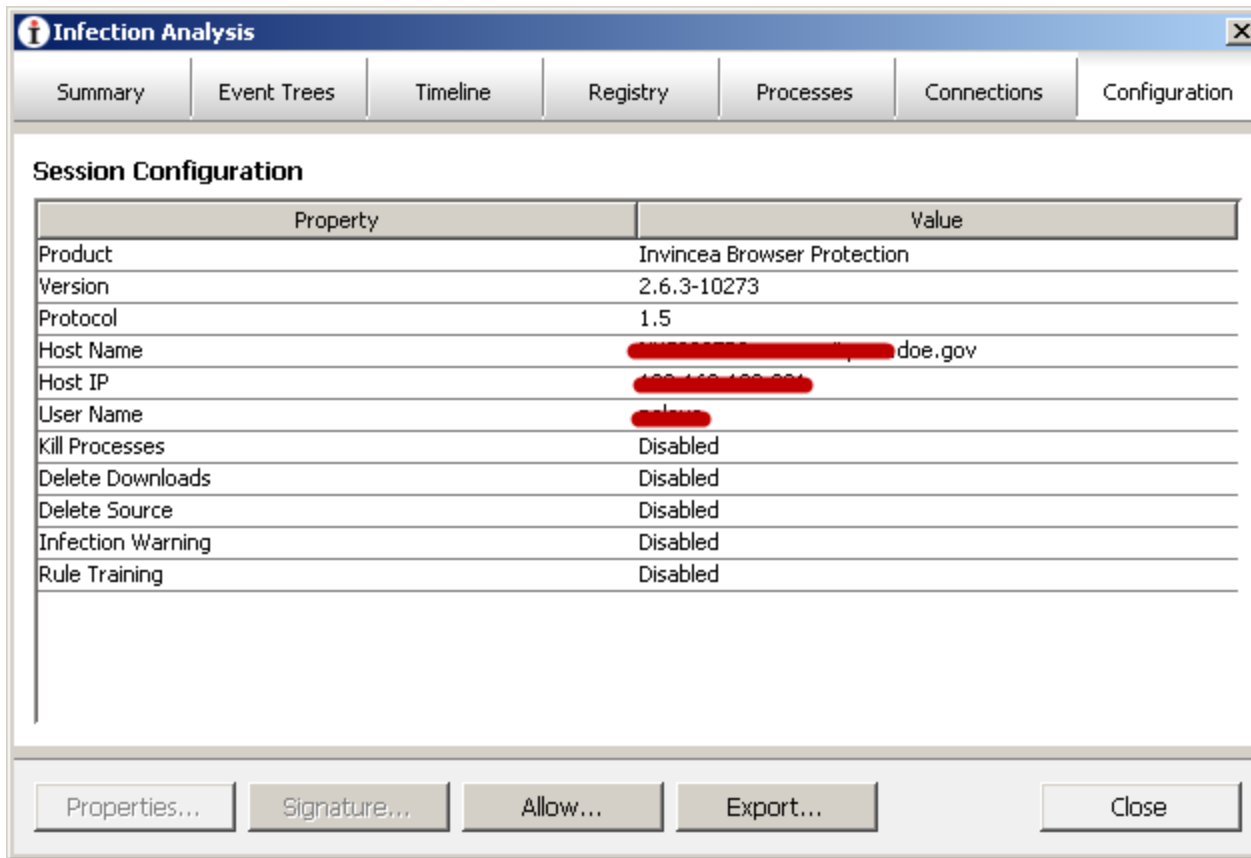
Protocol	Process (PID)	Address	State
UDP	youtube_video.scr (2332)	localhost:1103	Listening
TCP	youtube_video.scr (2332)		Connected
TCP	youtube_video.scr (2332)	ftp.pochta.ru:80	Connected
TCP	youtube_video.scr (2332)	web3.qip.ru:80	Connected
TCP	youtube_video.scr (2332)	m.iguiinho.com.br:80	Connected

At the bottom of the window, there are buttons for 'Properties...', 'Signature...', 'Allow...', 'Export...', and 'Close'.

- TCP Connected



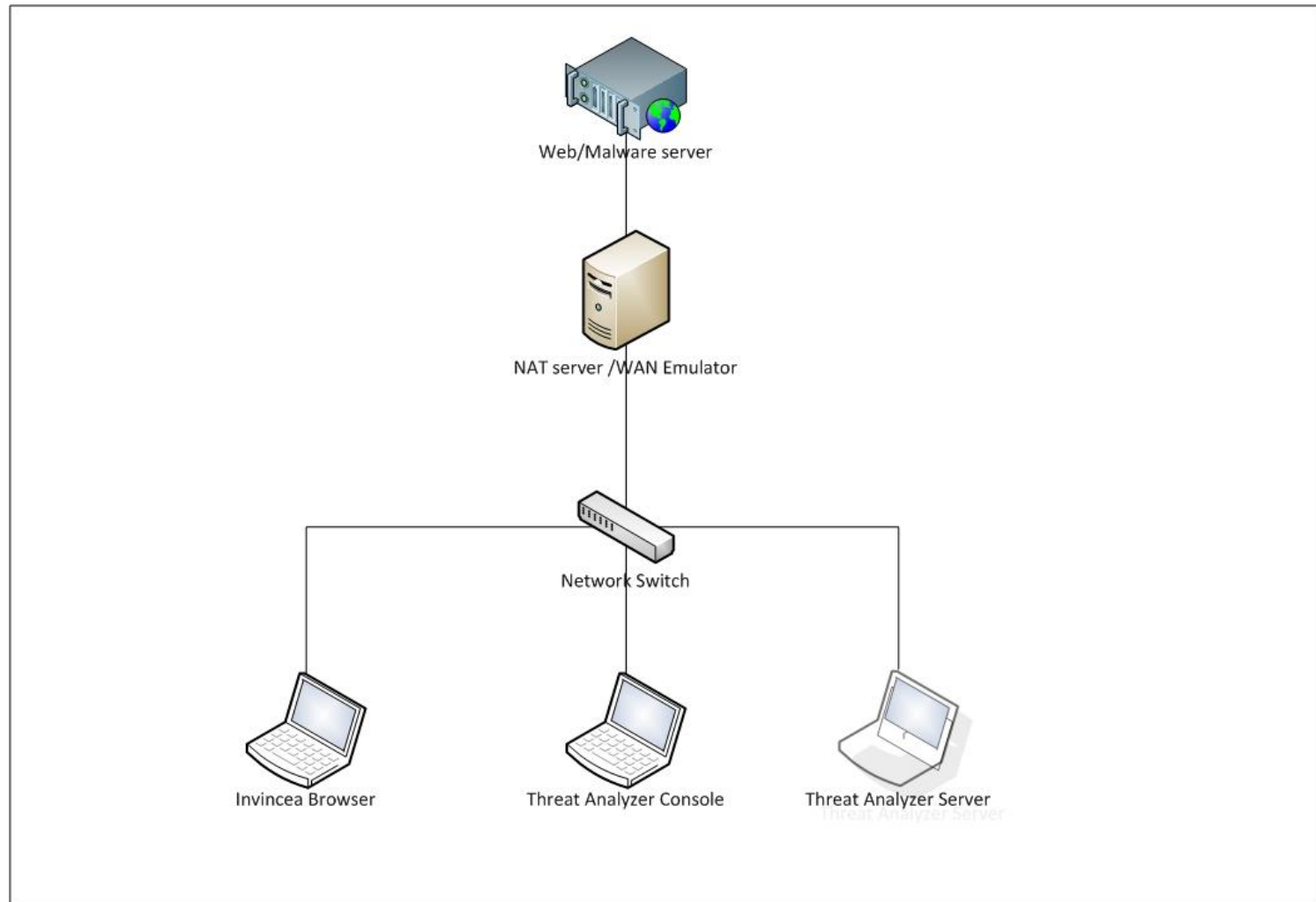
- Session Configuration



The image shows a screenshot of the 'Infection Analysis' window in the Invincea Threat Analyzer. The 'Configuration' tab is selected, displaying the 'Session Configuration' table. The table lists various properties and their values. Some values are redacted with black bars. At the bottom of the window, there are buttons for 'Properties...', 'Signature...', 'Allow...', 'Export...', and 'Close'.

Property	Value
Product	Invincea Browser Protection
Version	2.6.3-10273
Protocol	1.5
Host Name	[REDACTED] doe.gov
Host IP	[REDACTED]
User Name	[REDACTED]
Kill Processes	Disabled
Delete Downloads	Disabled
Delete Source	Disabled
Infection Warning	Disabled
Rule Training	Disabled

**Proof is in the
Pudding**



- Tested 10 different Case Related Malware Samples
- Introduced each via PDF, Drive-by or user initiated download
- Sniffed traffic leaving the machine once machine was exposed to malware
- Compared Results to Reverse Engineering Reports

IARC Test Results of “High Risk Malware”

Sample Name	Type	Malware Analysis / Attributes	Result
Sample 1	doc	<ul style="list-style-type: none"> Modified ACLs of files Executes file VBA script creates Docs_2.tmp Macro is protected by password of non-printable chars 	Blocked
Sample 2	tmp	<ul style="list-style-type: none"> Created or opened a file in the system directory Modified ACLs of files Changed time attribute of a specified file or directory Scheduled command and program to run Deleted itself after installation Executed a program using the cmd or bat method Installed a hook procedure Extracts syspol.exe and policy.dll from itself 	Blocked
Sample 3	exe	<ul style="list-style-type: none"> File when executed opens IE Injects itself into the IE process Attempts to download dd.exe Attempts to download 200512.exe Closes IE and executes downloads 	Blocked
Sample4	exe	<ul style="list-style-type: none"> Created or opened a file in the system directory Scheduled command and program to run Created or opened itself Set an autorun program Modified ACLs Extracts svchest.exe and svchest.reg to system folder Executes svchest.exe Executes regedit /s svchest.reg 	Blocked

IARC Test Results of “High Risk Malware”

Sample Name	Type	Malware Analysis / Attributes	Result
Sample 5	exe	<ul style="list-style-type: none"> Created or opened a file in the system directory Scheduled command and program to run Created or opened itself Set an autorun program Modified ACLs Extracts svchest.exe and svchest.reg to system folder Executes svchest.exe Executes regedit /s svchest.reg 	Blocked
Sample 6	exe	<ul style="list-style-type: none"> Created or opened a file in the system directory Modified ACLs Deleted itself after installation Scheduled command and program to run Opened or closed an existing service by handle Copied itself to another place Retrieved information about the next process Established connection to service control manager Packed file copies self to programfiles\netmeeting as hidden file launches IE and injects self in the process of IE 	Blocked
Sample 7	exe	<ul style="list-style-type: none"> Created or opened itself Created a mutex object Changed time attribute of a file or directory self-extracting archive that contains a script script is run after extraction 	Blocked
Sample 8	exe	<ul style="list-style-type: none"> Set an autorun program Modified ACLs Scheduled a command and program to run Deleted itself after installation contains strings with URL referencing backdoor.wmv 	Blocked

**ZERO SUCCESSFUL
MALWARE!**

Q & A

JERICH BEASON
BEASONJ@NV.DOE.GOV
(702)493-6011

SURAMIE RYAN
RYANS@NV.DOE.GOV
(702)408-5018